IN THE UNITED STATES DISTRICT COURT
DISTRICT OF UTAH

IN THE MATTER OF THE SEARCH OF TWO WHITE APPLE IPHONES SEIZED FROM LONG HOANG LUU.	Case No. 2:25mj256 JCB AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT Judge Jared C. Bennett

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Jeffrey Chmielewski, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent ("SA") with Homeland Security Investigations ("HSI"), assigned to the HSI Salt Lake City, Utah, office. I am concurrently assigned to the Utah Internet Crimes Against Children ("ICAC") Task Force, managed by the Utah Attorney General's Office, and the Child Exploitation Task Force ("CETF"), managed by the Salt Lake City Federal Bureau of Investigation ("FBI"). Prior to being employed by HSI, I was a Colorado State Patrol Trooper for approximately six years. My formal law enforcement training includes completing the Criminal Investigator Training Basic training course and the HSI Special Agent Training program at the Federal Law Enforcement Training Center in Glynco, Georgia. I have received additional training from CETF, ICAC, and other sources related to Child Sexual Abuse Material ("CSAM"), to

include child pornography (as defined in 18 U.S.C. § 2256), and exploitation investigations and specifically to online, undercover enticement.

2. I have been involved in investigations of federal criminal violations, including those related to the distribution, receipt, and possession of CSAM, child enticement and exploitation, and cybercrime. I have reviewed numerous examples of CSAM. I have become familiar with ways that CSAM is shared, stored, distributed, and/or produced, including the use of various social media websites (Facebook, Instagram, Twitter, Kik, Snapchat, Discord, etc.), messaging platforms and applications, electronic media storage, "cloud" based storage (Dropbox, Mega, Box, iCloud, etc.), and peer-to-peer ("P2P") networks. I have also become familiar with jargon or slang terms that people involved in child exploitation use to discuss their activities. I have gathered evidence pursuant to search warrants and have participated in searches of premises, persons, and electronic devices. I have conversed in undercover, online conversations with, and upon arrest, have interviewed persons who possess, view, and distribute CSAM or who seek to commit physical sexual offenses against minors.

3. As a federal agent, I am authorized to investigate violations of laws of the United States, and I am a law enforcement officer with the authority to execute warrants issued under the authority of the United States. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the search of a residence described in Attachment A.

PURPOSE OF THE AFFIDAVIT

4. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the search of two white Apple iPhones

(collectively the "SUBJECT CELLPHONES") found in the possession of Long Hoang LUU ("LUU"), described in Attachment A, for fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 2422(b) (Coercion and Enticement of a Minor), 18 U.S.C. § 2423(b) (Travel with intent to engage in illicit sexual conduct, 18 U.S.C. § 2251(a) (Attempted Production of Child Pornography), and 18 U.S.C. §§ 2252(a)(4) and 2252A(a)(5)(B) (Possession of Child Pornography), "collectively the SUBJECT OFFENSES", described in Attachment B.

5. The statements in this affidavit are based upon my personal observations, my training and experience, and information provided by law enforcement officers assigned to other law enforcement agencies, other special agents, and employees of HSI. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. Thus, I have not included each and every fact known to me concerning this investigation.

BRIEF SUMMARY

6. LUU is a Vietnamese citizen believed to be residing in Nevada and is a registered sex offender in the State of Texas (Registrations SR-07392848 and SR-595229730). According to his criminal record, LUU pleaded guilty to a Texas Felony 2 charge for "Indecency with a Child – Sexual Contact" and had several subsequent Texas charges for "Fail to Comply Sex Offenders Duty to Register", also resulting in a State of Texas Felony conviction.

7. Between approximately March 9, 2025, to March 15, 2025, LUU used online chat applications to communicate with someone he believed to be a 13-year-old female (MINOR) living in Salem, Utah. In fact, he was communicating with the fictitious persona of a Minor created by a law enforcement online covert employee (OCE). During the conversation, LUU repeatedly detailed his desire to engage in vaginal and oral sex with the MINOR, and asked if he could take

video of their sexual encounters. Ultimately, LUU made arrangements to meet the MINOR in person for sex. During the conversations, LUU sent a photograph of himself to MINOR and also indicated that he would be driving a White Jeep Grand Cherokee. On March 15, 2025, LUU traveled to Salem, Utah, to meet the MINOR, and was arrested. He matched the photograph send to the MINOR and was driving a White Jeep Grand Cherokee. At the time of his arrest, LUU had two white Apple iPhones in his vehicle. Further, there is probable cause to believe that LUU traveled from Nevada to Utah to meet the MINOR; his vehicle is registered to him at an address is Las Vegas, Nevada, and at the time of arrest, LUU possessed a Nevada driver's license with an address in Las Vegas, Nevada. As set forth below, there is probable cause to believe that evidence of the SUBJECT OFFENSES will be found on the SUBJECT CELLPHONES.

JURISDICTION

8. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A), and (c)(1)(A). Specifically, the Court is "a district court of the United States … that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

DEFINITIONS

9. Based on my training and experience, I use the following terms to convey the following meanings:

a. "Chat" is any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral

conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child Pornography" includes any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).

c. "Child Sexual Abuse Material" ("CSAM"): any use of the term "child sexual abuse material" or the acronym "CSAM" in this affidavit should be construed as a use of the term "child pornography" as defined is paragraph (a) above.

d. "Cloud-based storage service" refers to a publicly accessible, online storage provider that collectors of depictions of minors engaged in sexually explicit conduct can use to store and trade depictions of minors engaged in sexually explicit conduct in larger volumes. Users of such a service can grant access to their collections by sharing links, and associated passwords, to their stored files with other traders or collectors. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to a file stored on a cloud-based service does not need to be a user of the service to access the file. Access is readily available to anyone who has an internet connection.

e. "Computer" refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." *See* 18 U.S.C. § 1030(e)(1).

f. "Computer hardware" consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. "Computer passwords and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt,

compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

h. "Computer software" is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

i. "Electronic Service Provider" ("ESP") means any provider of electronic communication services or remote computing services.

j. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

k. "IP" stands for Internet Protocol. Internet Protocol provides the methodology for communication between devices on the Internet.

l. "Internet Protocol address" ("IP address") is a unique number that identifies a device on a computer network and is used by computers to move information on the Internet. Every device directly connected to the Internet must have a unique IP address.

m. "Internet Service Providers" are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

n. "Minor" means any person under the age of 18 years. *See* 18 U.S.C. § 2256(1).

o. "Mobile application" or "chat application" is a small, specialized program downloaded onto mobile devices, computers and other digital devices that enable users to perform a variety of functions, including engaging in online chat and sending or receiving images and videos.

p. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (including, but not limited to, phonograph records, printing, typing); or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic digital media.

q. "Remote computing service" is defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

r. "Sexually explicit conduct" applies to visual depictions that involve the use of a minor, *see* 18 U.S.C. § 2256(8)(A), or that have been created, adapted, or modified to appear to depict an identifiable minor, *see* 18 U.S.C. § 2256(8)(C). In those contexts, the term refers to actual or simulated (a) sexual intercourse (including genital-genital, oral-genital, or oral-anal), whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person. *See* 18 U.S.C. § 2256(2)(A).

s. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disk or other electronic means, which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

BACKGROUND ON COMPUTERS AND CHILD EXPLOITATION

10. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, I know that computers, computer technology, and the Internet have drastically changed how child pornography is produced and distributed.

11. Computers serve four basic functions in connection with child pornography: production, storage, communication, and distribution.

12. Child exploiters can upload images or video clips directly from a digital camera to a computer. Once uploaded, they can easily be edited, manipulated, copied, and distributed. Paper photographs can be transferred to a computer-readable format and uploaded to a computer using a

scanner. Once uploaded, they too can easily be edited, manipulated, copied, and distributed. A modem allows any computer to connect to another computer via a telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

13. The computer's ability to store images in digital form makes it an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive or more recently, memory) used in home computers has grown tremendously in the last several years. This storage can store millions of images at very high resolution. Images and videos of child pornography can also be stored on removable data storage media, such as external hard drives, thumb drives, media cards, and the like many of which are small, highly portable, and easily concealed, including on someone's person or inside their vehicle.

14. Computers, including mobile devices (cellphones), and mobile storage devices are highly capable, with numerous uses, including mapping, communication, instruction, and playing entertainment media and are often expensive. Moreover, these high-capability devices and easily portable upon a person, in bags or luggage, or in motor vehicles, vessels, trains, or airplanes. As such, travelers frequently travel with computers, including mobile devices (cellphones), and mobile storage devices.

15. The Internet affords collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion, including Internet Relay Chat, instant messaging programs such as Kik, bulletin board services, e-mail, "peer-to-peer" ("P2P") file-sharing programs such as LimeWire and eMule, and networks such as eDonkey, Gnutella, ARES, Tumblr, and BitTorrent. Collectors and distributors of child

pornography sometimes also use online resources such as "cloud" storage services to store and retrieve child pornography. Such online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in a variety of formats. A user can set up an online storage account from any computer with access to the Internet and can access stored files using any device capable of connecting to the Internet. Evidence of such online storage of child pornography is often found on the user's computer.

16. An Internet Protocol ("IP") address is a unique identifier that electronic devices such as computers, routers, fax machines, printers, and the like use to identify and communicate with each other over a network. An IP address can be thought of as a street address. Just as a street address identifies a particular building, an IP address identifies a particular Internet or network access device. When a user logs on to his/her Internet Service Provider ("ISP"), they are assigned an IP address for the purpose of communication over the network. The Internet Assigned Numbers Authority (IANA) manages the IP address space allocations globally. Internet Protocol version 4 (IPv4) defines an IP address as a 32-bit number while Internet protocol version 6 (IPv6) defines an IP address as a 128-bit number. Both versions are currently in use on the internet. These IP addresses can be written and displayed in human-readable notations, such as 192.0.2.1 in IPv4 and 2001:db8:0:1234:0:567:8:1 in IPv6.

17. An IP address can be statically assigned, meaning the IP address does not change from one Internet session to another, or dynamically assigned, meaning a user receives a different IP address each time the user accesses the Internet. The frequency in which this address changes is generally controlled by the Internet Service Provider and not the user.

18. A "dynamic" IP address means that the ESP assigns a different unique number to a device every time the device accesses the Internet. A "static" IP address means that the ESP assigns the same unique number to a device every time the device accesses the Internet.

19. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in the computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains P2P software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

RELATIONSHIP BETWEEN HANDS-ON CHILD SEXUAL OFFENDERS AND CHILD PORNOGRAPHY

20. I know, based on my training and experience, and based on conversations I have had with others who investigate child exploitation offenses, that people who have a sexual interest in children, including persons who commit hands on sexual offenses against children, and particularly those who travel to commit sexual offenses against children, often collect and trade in child pornography. These persons receive sexual gratification from images and video clips depicting the sexual exploitation of children.

21. I know that these persons may also use such images and videos to lower the inhibitions of children who they wish to sexually abuse, or to screen several children while seeking a possible victim. Such persons maintain their collections of child pornography in safe, secure, and private locations, such as their residence or vehicle, and on computers and digital storage media under their direct control. Such persons often maintain their collections, which are considered

prized possessions, for long periods of time, and prefer not to be without their collections for any prolonged period. In some cases, however, persons with a sexual interest in children have been found to download and delete child pornography on a cyclical and repetitive basis, rather than storing a collection of child pornography indefinitely.

22. I also know from my training and experience that many people who sexually exploit children often download child pornography from the Internet, and those who collect child pornography, frequently save images and videos of child pornography on their computers and/or transfer copies to other computers and storage media, including cloud storage accounts, external hard drives, thumb drives, flash drives, SD cards, and CDs or DVDs. Moreover, it is common in child exploitation investigations to find child pornography on multiple devices and/or storage media located in suspects' homes, rather than on a single device.

23. I know based on my training and experience that many social media and messaging platforms, such as Facebook, Instagram, Twitter, Snap Chat, Kik messenger, and others can be directly accessed and used with one's cellular phone. Often, these applications require the user to download the application directly to their phone, which then allows seamless use between the cellular phone and the social media or messaging website.

BACKGROUND ON SOCIAL MEDIA PLATFORM A[1]

24. Social Media Platform A is a chat messenger app for mobile devices such as tablets and smartphones. Users can also exchange media with each other. Social Media Platform A advertises itself as secure and anonymous and allows users to chat in groups while concealing their

[1] Social Media Platforms A and B are known to law enforcement and are intentionally omitted to protect ongoing investigations on those platforms. The name of the social media platforms will be provided to anyone assisting in the search of the devices and to the Court upon request.

identity and keeping conversations private, using self-destructing messages to make communications temporary. The platform advertises that it can be used for anonymous dating and adult conversations as well as roleplaying activities, offering a space for users to explore different interactions and scenarios.

BACKGROUND ON SOCIAL MEDIA PLATFORM B[1]

25. Social Media Platform B is an app for mobile devices such as tablets and smartphones that allows users to chat and share files or websites with other users over the internet. It generates user accounts based on usernames, unlike similar services that use phone numbers, which allows users to restrict with whom they communicate.

26. Users can also exchange images, videos, and other files with each other. Users can designate themselves as a group with an identifying name, which allows the users to communicate and share files with all the members of the group simultaneously. Users can share files stored on their individual device by selecting the share or attach function and then selecting the source or storage location of the file. This includes storage locations like the Gallery or Camera, which are apps or features of a smartphone that are capable of storing and organizing digital images and videos.

27. The Social Media Platform B app stores chats and messages on the user's device. For iOS devices, which includes Apple, Inc., and products such as an iPhone or iPad, the app will store the last 1,000 messages from a chat occurring within the last 48 hours, and the last 500 messages for older chats. For an Android device, which the operating system for most mobile devices that are not Apple products, the app will store the last 600 messages in a chat within the last 48 hours, and then the last 200 messages for older chats. Users can also send images and videos

that are stored on their devices to other users via the app and can save or download files sent to them through the app to their devices

28. A user can create either a public group or a private group with the app. To start a private group, a user adds members from a private list of friends or contacts. A user creates a public group by setting a name, photo, and username of the group. This allows other users on the app to find and participate in the group by searching for a certain keyword. The user who started the group can also change the name of the groups as it displayed on other users' phones, called the display name.

STATEMENT OF PROBABLE CAUSE

A. Meeting on Social Media Platform A

29. On Sunday, March 9, 2025, the law enforcement OCE, hereinafter referred to as MINOR, posted "Hi everyone! F here" in the Social Media Platform A Utah Chat Group. The MINOR received several private messages wishing to chat, including one from username ZD, who was subsequently identified as and is hereinafter referred to as LUU.

30. LUU began the private conversation with "Hello female".[2] After exchanging pleasantries, LUU asked if the MINOR is from Utah and offered that he is from St. George. LUU offered "Good chance we could meet if we are close", to which the MINOR responded "so I gotta tell u Im only 13. guys usually bounce when i tell them that". LUU responded that is fine and that they are just talking. LUU quickly asked for a physical description of the MINOR. The OCE described the MINOR as small and slim, and then sent LUU and image of an adult digitally altered

[2] Punctuation is intentionally outside of quoted chat messages and typos are included to preserve the accuracy of the quoted messages.

to appear to be a 13-year-old girl.

31. As the conversation continued, LUU stated his age was 36 (in fact LUU is 49 years old). The MINOR explained that she lived alone with her grandmother. LUU ask several questions about the MINOR's prior date experience, including the age of her ex-boyfriend, and how they had met. The MINOR offered that her ex-boyfriend was an adult who she had met online. When asked if he likes younger, LUU responded "I love young". LUU also stated "I want a young girl to be my little girl", and "It's a fetish of mine", "I like a sweet innocent girl", and "I would if you let me be your daddy". LUU directs "I want you to sneak out", and when asked "wut would u want to do?", LUU offered "We could fuck if you want".

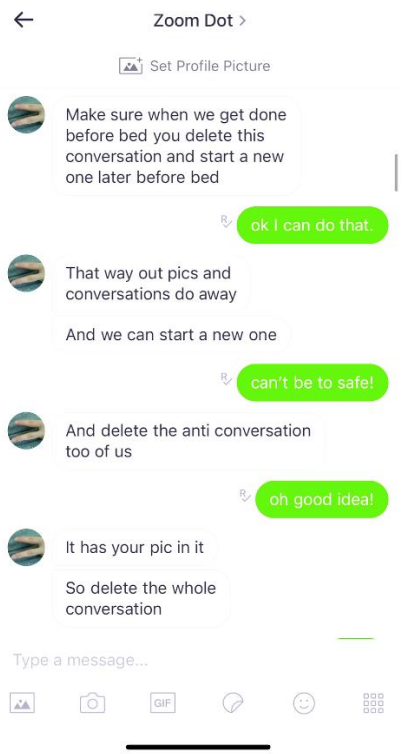
32. The MINOR agreed and offered a coming date when her grandmother would be out of town, leaving the MINOR alone at home. LUU asked if they could use the MINOR's bed and stated "Good no condom though. I want to feel you" and in response to another reference request about not getting pregnant, … "I'll pull out but you have to let me cum in your mouth". When the MINOR responded she had never had anyone "cum" in her mouth and that it makes her nervous LUU responded "Okay lets just see how you feel at the time". The conversation continued for a short time before moving to Social Media Platform B, where LUU used the username "Zoom Dot".

B. Conversation on Social Media Platform B and request to Video Record the Rape

33. Once on Social Media Platform B, LUU began asking the MINOR to call him "daddy." The MINOR provided a general meeting location.[3] LUU asked the Minor what she would wear and ultimately requested pigtails and a hoody and shorts with knee high socks. LUU stated

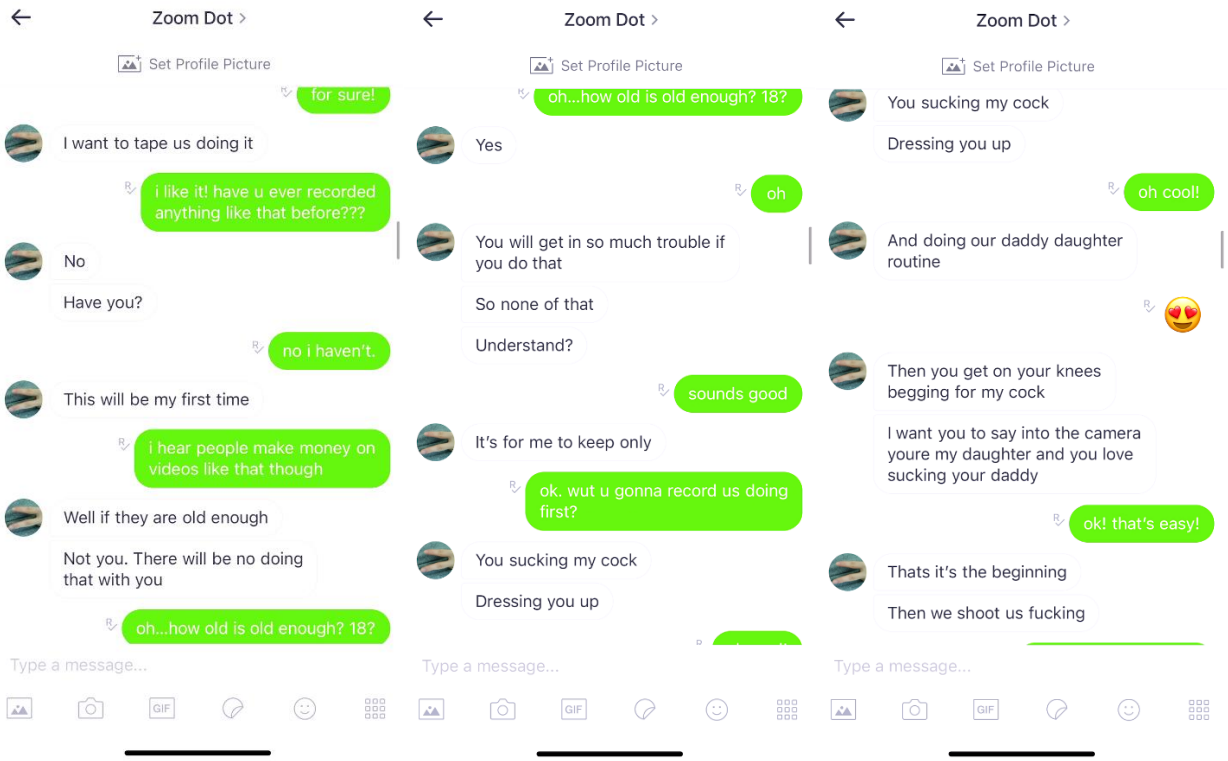
[3] Due to rolling message limits in the Social Media Platform B app, approximately one day of this conversation was not preserved by the investigator. A separate search warrant will be sought for Social Media Platform B to attempt to retrieve these messages.

"This is like exciting" and directed the MINOR to delete the conversation and start a new one because "That way out pics and conversations do away". LUU also directed "And delete the [Social Media Platform A] conversation too of us", "It has your pic in it", "So delete the whole conversation", and "I am glad that you are cautious this makes me feel better."



34. At several different points in the conversation, LUU asked the MINOR to delete the conversation, indicating that he knew what he was doing was illegal and could get him into trouble. LUU repeatedly directed the usage of "daddy" and "daughter" titles and stated, "I want to teach you and help you explore what it's like". LUU asked several times to see photos of the MINOR's closet so he could pick out the clothes he wanted MINOR to wear for their meeting. The OCE sent LUU several photos of clothing that was age-appropriate for a 13-year-old girl.

35. After additional conversation about outfits, LUU stated "I want to try everything", "I want to make a video of us", "I told you it's has to be a secret", "and "I want to tape us doing it". When the MINOR stated, "I hear people make money on videos like that though", LUU responded "Well if they are old enough" and "Not you. There will be no doing that with you". When the MINOR asked "oh…how old is old enough? 18?", LUU responded "Yes", "You will get in so much trouble if you do that", "So none of that", "Understand?" and "Its for me to keep only". When asked what LUU wanted to record first, he replied "You sucking my cock" and subsequently "I want you to say into the camera youre my daughter and you love sucking your daddy", and "That's it's the beginning", and "Then we shoot us fucking".



36. When the MINOR asked, "how do u record that?", LUU responded "With my phone", and "I'll just set it on the desk", and "Yes and holding it to get close up", and added, "I

want you to look into the camera and say your age too". Based on my training and experience, and the plain language of these chats, LUU was telling MINOR that he intended to produce child pornography of her engaging in sexual activity with him. He also made it clear that he understood the MINOR to be 13 years old, and that if he were caught he would be in a lot of trouble.

37. LUU stated "I want you to fantasize that im your real dad ok", and "Then tell me you love me", and "I want it to be like incest".

38. In the conversation, the MINOR repeatedly discussed topics that were appropriate for a 13-year-old, such as the fact that she lived with her grandma, went to school, that she rides to school on an electric scooter. She also sent a second photograph depicting an adult, digitally modified photo to appear to be 13-year-old girl, standing in front of a whiteboard in a school classroom. LUU offered to help the MINOR with some math homework. When asked, LUU stated his first name is "Luu" then immediately corrects it to "Lou" but asked to continue to be called "daddy."

39. LUU stated his family lives in "Vegas" and then stated that he lives really close to "Vegas." LUU stated that he drives a white Jeep Grand Cherokee.

40. When LUU asks "What kind of panties will you wear", the MINOR asks LUU if he could bring some. LUU responded "I'll bring you a thong", and "What size do you wear". LUU also offered to get the MINOR a Red Bull energy drink as LUU stated, "I need you to stay awake all night if you can".

41. LUU directed the MINOR to masturbate with very specific instruction. LUU stated "I might stick it in right when I get in the door and do it at the front door". Later in the conversation, LUU stated that he was scared, and clarified that he was not scared of the MINOR, stating, "No

but in anyone find out lol", and "I worry a neighbor you know", and "Let's make sure it's dark", "and "Is there a back way out just in case".

42. Discussing their upcoming plans to meet, LUU made several additional statements about "raping" the MINOR and directed the MINOR to "… get nice and clean and make yourself presentable", and "Don't forget the pigtails", because "That's very important understand". They made plans to meet at a designated place in Salem, Utah.

C. LUU Travels to Salem, UT and Investigators find the SUBJECT CELLPHONES

43. On Friday, March 14, 2025, at approximately 6:45 PM, LUU told the MINOR he purchased her something and sent a photo of a white bra and of black underwear on the black seat of a vehicle. LUU asked the MINOR if she showered, ate, and brushed her teeth. By 8:02 PM, when asked, LUU reported that he was on the road, and at approximately 8:57 PM, LUU reported "I'm like 3 hrs away", and that he would be there around "12". LUU gave continued time updates at 1.5 hours, 45 minutes, and 30 minutes, and 15 minutes away. LUU again messaged the MINOR when he parked.

44. On March 15, 2025, at approximately 12:05 AM, investigators observed as a white Jeep Grand Cherokee pulled into the arranged meeting location established by investigators and parked. At the same time, the OCE received the message from LUU stating, "O jus parked". Investigators approached and arrested LUU, observing that LUU matched the photo he had sent to the MINOR in the chat conversations.

45. In the vehicle investigators found a Walmart shopping bag containing bra and underwear LUU had sent photos of and said he had purchased for the MINOR as well as several cards for Las Vegas casinos. Investigators found the SUBJECT CELLPHONES within arm's reach

of the driver's seat. The SUBJECT CELLPHONES were powered on and one iPhone had navigation directions to the meeting location established by the OCE.

46. During a subsequent interview of LUU, LUU provided an address in Arizona and elected not to answer any questions.

D. There Is Probable Cause to Believe the Items Listed in Attachment B Will Be Located on the SUBJECT CELLPHONES

47. The Jeep Grand Cherokee LUU drove to the meeting location has Nevada license plates and is registered to LUU in Las Vegas, while the Nevada driver's license in LUU's wallet also has a Las Vegas address. Each street address is on the west side of Las Vegas, in the Spring Valley area. A review of law enforcement databases shows LUU to have an established presence at the driver's license address from 2014 to 2015, and at the address of the vehicle registration from 2017 to present. A review of law enforcement records of license plate readings shows the license plate on the Jeep Grand Cherokee in the Las Vegas metro area dozens of times within the past 30 days, as recently as March 14, 2025, at 8:52 AM PDT, the morning of the day LUU traveled to Utah. Thus, there is probable cause to believe that LUU traveled to Utah from Nevada in order to engage in illicit sexual activity with the MINOR.

48. Further, as set forth above, there is probable cause to believe that LUU intended to produce child pornography upon meeting the minor. LUU specifically stated several times what he wanted to video record, that he wanted to use his phone to record it, and that they would get in big trouble if they shared it with anyone.

49. I know from training and experience that suspects engaged in enticement conversations with minors will sometimes misreport facts about themselves to seem more

approachable to their victim. In this case, LUU misrepresented his age, and appeared to misrepresent his location. I also know from training and experience that suspects engaged in enticement conversations with minors who express a desire to record the rape or sodomy of a child often have a predisposition to create, collect, and store CSAM. As such, there is probable cause to believe that evidence of LUU's communications with the MINOR, geolocation data of LUU prior to and during his travel to meet with the minor, and evidence of CSAM is contained in the SUBJECT CELLPHONES.

SEARCH AND SEIZURE OF DIGITAL DATA

50. This application seeks permission to search for and seize evidence of the crimes described above, including evidence of how computers, digital devices, and digital storage media were used, the purpose of their use, and who used them.

51. Based on my training and experience, and information related to me by agents and others involved in the forensic examination of computers and digital devices, I know that data in digital form can be stored on a variety of systems and storage devices, including hard disk drives, floppy disks, compact disks, magnetic tapes, flash drives, and memory chips. Some of these devices can be smaller than a thumbnail and can take several forms, including thumb drives, secure digital media used in phones and cameras, personal music devices, and similar items.

52. I know from my training and experience, as well as from information found in publicly available materials, that these digital devices offer their users the ability to unlock the device via the use of a fingerprint, thumbprint, or facial recognition in lieu of a numeric or alphanumeric passcode or password. These features are commonly referred to as biometric authentication and their availability is dependent on the model of the device as well as the operating

system on the device. If a user enables biometric authentication on a digital device, he or she can register fingerprints, or his or her face, to unlock that device.

53. In some circumstances, biometric authentication cannot be used to unlock a device, and a passcode or password must be used instead. These circumstances include: (1) the device has been turned off or restarted; (2) the device has received a remote lock command; (3) too many unsuccessful attempts to unlock the device via biometric authentication are made; (4) too many hours have passed since the last time the device was unlocked; and (5) the device has not been unlocked via biometric authentication for a period of time and the passcode or password has not been entered for a certain amount of time. Thus, in the event law enforcement encounters a locked digital device, the opportunity to unlock the device via biometric authentication exists only for a short time.

54. The passcode or password that would unlock any devices at the SUBJECT PREMISES is not known to law enforcement. Thus, it is necessary to press the fingers of FOWLER to any phones device's sensor, or hold the phone up to FOWLER's face, in an attempt to unlock the devices for the purpose of executing the search authorized by this warrant. Attempting to unlock the relevant device(s) via biometric authentication is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant. I therefore request that the Court authorize law enforcement officers to press the fingers, including thumbs, of FOWLER to the fingerprint sensor of any phones or digital devices equipped with fingerprint authentication, or to hold the device equipped with facial recognition authentication up to FOWLER's face, to unlock the device and thereby allow investigators to search the contents as authorized by this warrant.

REMOVAL AND FORENSIC IMAGING OF DATA STORAGE DEVICES

55. A forensic image is an exact physical copy of a data storage device. A forensic image captures all data on the subject media without viewing or changing the data in any way. Absent unusual circumstances, it is essential that a forensic image be obtained prior to conducting any search of data for information subject to seizure pursuant to the warrant. During a search of premises it is not always possible to create a forensic image of or search digital devices or media for data for various reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. Because there are so many different types of digital devices and software in use today, it is difficult to anticipate all the necessary technical manuals, specialized equipment, and specific expertise necessary to conduct a thorough search of the media to ensure that the data will be preserved and evaluated in a useful manner.

b. Searching digital devices can require the use of precise, scientific procedures designed to maintain the integrity of the evidence and to recover latent data not readily apparent to the casual user. The recovery of such data may require the use of special software and procedures, such as those used in a law enforcement laboratory.

c. The volume of data stored on many digital devices is typically so large that it is generally highly impractical to search for data during the execution of a physical search of premises. Storage devices capable of storing several terabytes of data are now commonplace in desktop computers. It can take several hours, or even days, to image a single hard drive; the larger the drive, the longer it takes. Even portable storage devices

such as memory cards and USB and flash drives can have capacities of 256 or 512 gigabytes or more. Depending upon the number and size of the devices, the length of time that agents must remain onsite to image and examine digital devices can make doing an on-site search impractical.

LABORATORY SETTING MAY BE ESSENTIAL FOR COMPLETE AND ACCURATE ANALYSIS OF DATA

56. Since digital data may be vulnerable to inadvertent modification or destruction, a controlled environment, such as a law enforcement laboratory, may be essential to conduct a complete and accurate analysis of the digital devices from which the data will be extracted. Software used in a laboratory setting can often reveal the true nature of data. Therefore, a computer forensic reviewer needs a substantial amount of time to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband, or an instrumentality of a crime.

57. Analyzing the contents of a computer or other electronic storage device, even without significant technical difficulties, can be very challenging, and a variety of search and analytical methods must be used. For example, searching by keywords, which is a limited text-based search, often yields thousands of hits, each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant hit does not end the review process. The computer may have stored information about the data at issue which may not be searchable text, such as: who created it; when and how it was created, downloaded, or copied; when it was last accessed; when it was last modified; when it was last printed; and when it was deleted. The relevance of this kind of data is often contextual. Furthermore, many common email, database, and spreadsheet applications do not store data as

searchable text, thereby necessitating additional search procedures. To determine who created, modified, copied, downloaded, transferred, communicated about, deleted, or printed data requires a search of events that occurred on the computer in the time periods surrounding activity regarding the relevant data. Information about which users logged in, whether users shared passwords, whether a computer was connected to other computers or networks, and whether the users accessed or used other programs or services in the relevant time-period, can help determine who was sitting at the keyboard.

58. *Latent Data*: Searching digital devices can require the use of precise scientific procedures designed to maintain the integrity of the evidence and to recover latent data. The recovery of such data may require the use of special software and procedures. Data that represents electronic files or remnants of such files can be recovered months or even years after it has been downloaded onto a hard drive, deleted, or viewed via the Internet. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in space on the hard drive or other storage media that is not allocated to an active file. In addition, a computer's operating system may keep a record of deleted data in a swap or recovery file or in a program specifically designed to restore the computer's settings in the event of a system failure.

59. *Contextual Data*:

a. In some instances, the computer "writes" to storage media without the specific knowledge or permission of the user. Generally, data or files that have been

received via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to such data or files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve artifacts of electronic activity from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer usage. Logs of access to websites, file management/transfer programs, firewall permissions, and other data assist the examiner and investigators in creating a "picture" of what the computer was doing and how it was being used during the relevant time in question. Given the interrelationships of the data to various parts of the computer's operation, this information cannot be easily segregated.

b. Digital data on the hard drive that is not currently associated with any file may reveal evidence of a file that was once on the hard drive but has since been deleted or edited, or it could reveal a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, email programs, and chat programs store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, can indicate the identity of the user of the

digital device, or can point toward the existence of evidence in other locations. Such data may also lead to exculpatory evidence.

c. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be learned from the absence of particular data on a digital device. Specifically, the lack of computer security software, virus protection, malicious software, evidence of remote control by another computer system, or other programs or software, may assist in identifying the user indirectly and may provide evidence excluding other causes for the presence or absence of the items sought by this application. Additionally, since computer drives may store artifacts from the installation of software that is no longer active, evidence of the historical presence of the kind of software and data described may have special significance in establishing timelines of usage, confirming the identification of certain users, establishing a point of reference for usage and, in some cases, assisting in the identification of certain users. This data can be evidence of a crime, can indicate the identity of the user of the digital device, or can point toward the existence of evidence in other locations. Such data may also lead to exculpatory evidence. Evidence of the absence of particular data on the drive is not generally capable of being segregated from the rest of the data on the drive.

SEARCH PROCEDURE

60. In searching for data capable of being read, stored, or interpreted by a computer or storage device, investigators executing the search warrant will employ the following procedure:

a. *On site search, if practicable*. Law enforcement officers trained in computer forensics (hereafter, "computer personnel"), if present, may be able to determine if digital

devices can be searched on site in a reasonable amount of time and without jeopardizing the ability to preserve data on the devices. Any device searched on site will be seized only if it contains data falling within the list of items to be seized as set forth in the warrant and in Attachment B.

b. *On site imaging, if practicable*. If a digital device cannot be searched on site as described above, the computer personnel, if present, will determine whether the device can be imaged on site in a reasonable amount of time without jeopardizing the ability to preserve the data.

c. *Seizure of digital devices for off-site imaging and search*. If no computer personnel are present at the execution of the search warrant, or if computer personnel that are on-site determine that a digital device cannot be searched or imaged on site in a reasonable amount of time and without jeopardizing the ability to preserve data, the digital device will be seized and transported to an appropriate law enforcement laboratory for review.

d. *Manual review of devices may be necessary*. Some applications installed on devices or data stored on devices may not be able to be forensically imaged or viewed. Such factors may include but are not limited to unique encryption applications or protocols, installed digital rights management services (DRM) to restrict a device or protect content, or customized or beta versions of applications. In such cases this data will be be reviewed or obtained via a manual search of the device where an investigator operates device in the same way that an owner or other user would.

e. Investigators will examine the digital device to extract and seize any data that falls within the list of items to be seized as set forth in the warrant and in Attachment B. To the extent they discover data that falls outside the scope of the warrant that they believe should be seized (e.g., contraband or evidence of other crimes), they will seek an additional warrant.

f. Investigators will use procedures designed to identify items to be seized under the warrant. These procedures may include the use of a "hash value" library to exclude normal operating system files that do not need to be searched. In addition, investigators may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data falls within the list of items to be seized under the warrant.

g. In order to conduct a thorough search for inculpatory and exculpatory evidence, investigators may need to review evidence over time or with various forensic tools. It is impractical for the government to review the forensic data from each device simultaneously. Moreover, various pieces of evidence recovered from digital devices may have unknown probative value until they are considered within the context of additional evidence found in the ongoing investigation. In order to comprehend the facts in sum, investigators will maintain access to all evidence and may need to reexamine any particular piece of evidence as it was originally preserved.

h. If an original digital device does not contain any data falling within the list of items to be seized pursuant to this warrant, the government will return that original data device to its owner within a reasonable time following the search of that original data device and will seal any image of the device, absent further authorization from the Court.

RETENTION OF IMAGE

61. The government will retain a forensic image of each electronic storage device subjected to analysis for a number of reasons, including proving the authenticity of evidence to be used at trial; responding to questions regarding the corruption of data; establishing the chain of custody of data; refuting claims of fabricating, tampering with, or destroying data; and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

CONCLUSION

62. Based upon the foregoing, I have probable cause to believe that Long Hoang LUU committed the SUBJECT OFFENSES and that contraband and evidence, fruits, and instrumentalities of those violations, as described in Attachment B, will be located in the SUBJECT CELLPHONES, as described in Attachment A.

*/s/ _Jeffrey Chmielewski*_____
JEFFREY M. CHMIELEWSKI
Special Agent
Homeland Security Investigations

Sworn to before me telephonically or by other reliable means pursuant to Fed. R. Crim. P. 4.1 at 4:10 pm on March 18th, 2025.

JARED C. BENNETT
United States Magistrate Judge